

AES: HDM
F. #2018R0422

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
HARRIS@TRADEANEDGE.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF A PROVIDER
(EMAIL ACCOUNT)**

Case No. 18-M-523 _____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Christine Cullen, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account HARRIS@TRADEANEDGE.COM (the "TARGET ACCOUNT") that is stored at premises controlled by Google, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector with the United States Postal Service, and have been since 2017. During my career as a federal law enforcement officer, I have personally participated in numerous investigations and arrests, the debriefing of witnesses, and the execution of numerous search warrants related to various types of criminal activity including, among others, wire fraud, as well as search warrants related to electronically stored information.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1341 (wire fraud), 1348 (commodities fraud) and 1512(c)(2) (obstruction of justice) have been committed by Harris Landgarten. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband and/or fruits of these crimes, further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Since at least July 2014 through at least March 2017 (the “Relevant Time Period”), Harris Landgarten (“Landgarten”), while acting as a commodity pool operator (“CPO”), engaged in a scheme to fraudulently obtain money from a commodity pool he operated, the Tradeanedge Members Fund (“TMF” or the “Fund”). During the Relevant Time

Period, Landgarten operated the Fund out of his residence in the Eastern District of New York. Landgarten would incur purported Fund expenses and then withdraw money from the Fund to reimburse himself for these expenses, without ever disclosing either the purported expenses or the reimbursement withdrawals to the three investors who participated in the Fund (“TMF Participants”). During the Relevant Period, Landgarten wrongfully obtained approximately \$80,000 from TMF Participants through this scheme.

7. Rather than disclose that he was incurring purported expenses and using pool participants’ funds to pay for the purported Fund expenses, Landgarten instead misrepresented to TMF Participants—on statements he prepared and provided by e-mail using the TARGET ACCOUNT—that their investments were worth an amount that included the funds he had already spent. For example, on or about May 8, 2016, Landgarten used the TARGET ACCOUNT to e-mail a balance statement to John Doe #1, one of the TMF Participants. The balance statement indicated that John Doe #1 had a remaining balance of \$33,366.88 in the Fund on March 31, 2016 when, in reality, the Fund as a whole had only \$28,680.95 in assets on March 31, 2016.

8. Over the course of the Relevant Period, as Landgarten continued to withdraw money from the Fund, the value of the TMF Participants’ investments as reflected on the statements prepared by Landgarten diverged further and further from the amount of money actually in the Fund. Eventually, in or around October 2016, while he continued to represent to TMF Participants that, collectively, their investments were worth approximately \$80,000, the Fund had only approximately \$8,000 in its accounts. Landgarten claimed the entire \$8,000 was owed to him for unreimbursed expenses, and failed to use the remaining \$8,000 to honor a

participant's withdrawal request. Thus, for TMF Participants, the value of the Fund was effectively zero.

9. In addition, on or about March 31, 2016, John Doe #1 e-mailed Landgarten at the TARGET ACCOUNT a written notice of withdrawal of John Doe #1's investment in the Fund. In approximately April 2016 and May 2016, Landgarten promised to wire John Doe #1 \$33,366.88, a sum that Landgarten falsely represented to be the value of John Doe #1's remaining assets in the Fund on March 31, 2016. Landgarten wired \$1,000 to John Doe #1. However, Landgarten never wired the remaining balance of \$32,366.88 to John Doe #1.

10. On or about May 19, 2016, John Doe #1 filed a complaint against Landgarten with the Financial Industry Regulatory Authority ("FINRA") and the National Futures Association ("NFA"), in connection with Landgarten's refusal to return John Doe #1's investment in the Fund. FINRA and NFA referred the matter to the Commodity Futures Trading Commission ("CFTC"). On or about August 17, 2016, the CFTC initiated a formal investigation into Landgarten's conduct, entitled "Landgarten, Harris; Tradeanedge Members Fund L.P." (the "CFTC Proceeding"), with authority to issue subpoenas, pursuant to an Omnibus Order, entitled "In Re Certain Persons Engaged in Fraud with Respect to Pooled Investments and/or Managed Accounts." As part of the CFTC Proceeding, the CFTC served Landgarten with subpoenas for documents and testimony regarding the Fund. On or about October 5, 2016, pursuant to a CFTC subpoena, Landgarten provided in-person testimony to officers of the CFTC at the CFTC's offices in New York, New York.

11. Between approximately January 2017 and March 2017, during the CFTC Proceeding, Landgarten and officers of the CFTC communicated multiple times, by telephone and e-mail, using the TARGET ACCOUNT, about a potential settlement. While Landgarten was

communicating with the CFTC, he also contacted John Doe #1 by telephone and e-mail, using the TARGET ACCOUNT. On or about and between approximately March 7, 2017 and March 10, 2017, Landgarten proposed to John Doe #1, in Skype calls and e-mails, using the TARGET ACCOUNT, that John Doe #1: (a) withdraw his complaint from the CFTC, and (b) file an affidavit with the CFTC stating that John Doe #1 was “not deceived or defrauded or in any way misled” by the defendant. Landgarten further asserted that Landgarten would return John Doe #1’s purported \$33,366.88 investment in the Fund only if John Doe #1 withdrew his CFTC complaint against Landgarten. On or about March 10, 2017, John Doe #1 rejected Landgarten’s demands.

12. On July 2, 2018, a preservation request was sent to Google for the TARGET ACCOUNT. In general, an email that is sent to a Google subscriber is stored in the subscriber’s “mail box” on Google’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google’s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google’s servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

13. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts, like the email account listed in Attachment A, which Google hosts for the subscriber. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning

subscribers and their use of Google services, such as account access information, email transaction information and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

15. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP

address information can help to identify which computers or other devices were used to access the email account.

16. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

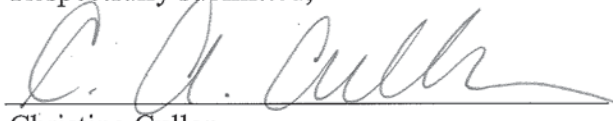
17. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can

understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

18. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Christine Cullen
Postal Inspector
United States Postal Service

Subscribed and sworn to before me on July 9, 2018



HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with HARRIS@TRADEANEDGE.COM that is stored at premises owned, maintained, controlled or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on July 2, 2018, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account that were sent, received or created between and including July 1, 2014 and March 31, 2017, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized; and
- d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 1341 (wire fraud), 1348 (commodities fraud) and 1512(c)(2) (obstruction of justice), involving Harris Landgarten and occurring on or after July 1, 2014, including, for the account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications between Landgarten and TMF Participants, including John Doe #1; communications between Landgarten and officers and employees of the Commodity Futures Trading Commission; preparatory steps taken in furtherance of the scheme; and payment of undisclosed expenses;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and
- (e) The identity of the person(s) who communicated with the user ID about matters relating to commodities fraud, wire fraud and obstruction of justice, including records that help reveal their whereabouts.